Notice of Allowability	Application No.	Applicant(s)	
	10/759,623	GARDNER ET AL.	
	Examiner	Art Unit	
	Jacob F. Betit	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed 7/15/2011, suplimental response filed 8/8/2011, and Interview dated 9/12/2011*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1,3-7,9 and 23-36*.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

   Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
   THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 12/31/2010
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20110912* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Jacob F Betit/
Primary Examiner, Art Unit 2169

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Reena Kuyper, Reg. No. 33,830 on 12 September 2011.

2. The application has been amended as follows:

The following listing of claims should replace all others:

1. (Currently Amended) A method of extracting original data from at least one file that resides on one or more different mediums operating on one or more different platforms, wherein the original data is extracted and stored at a target location without unnecessary replication of duplicate data, comprising the steps of:

obtaining content data and metadata relating to the original data of the at least one file, wherein the at least one file is stored in a first environment created on the one or more different mediums operating in the one or more different platforms;

in a second environment created on the one or more different mediums operating in the one or more different platforms and the target location, storing the content data and the metadata of the at least one file, wherein the content data is associated with the metadata, and wherein the second environment is different from the first environment;

obtaining an original location corresponding to the at least one file, the original location indicative of where the at least one file is stored in the first environment;

in the second environment, storing the original location in a location table, wherein the location table includes the following:

a link to the content data stored in a content hash table, indexed in response to the original location indicative of where the at least one file was stored in the first environment; and

a link to the metadata stored in a metadata hash table, indexed in response to the original location where the file was stored in the first environment;

reconstituting at least a piece of the at least one file by accessing at least one of the following in the location table:

the link to the content data, in response to the original location; and

the link to the metadata, in response to the original location; and

storing the content data in ~~a~~ the content hash table and the metadata in ~~a~~ the metadata hash table, wherein the storing operation further comprises the steps of;

generating a digital signature from the content data; and

utilizing the digital signature to compare the content data of the least one file that is being extracted with content data already resident at the target location to avoid replication of content data and only storing content data that is not duplicative of the content data that is already resident at the target location.

2. (Cancelled)

3. (Currently amended) The method of claim [[2]] 1, wherein the step of storing the content and metadata further comprises the steps of:

generating a digital signature from the metadata;

storing the content in an entry in the content hash table, wherein the content's digital signature is an index into the content hash table, so that the content's digital signature is the link to the content; and

storing the metadata in an entry in the metadata hash table, wherein the metadata's digital signature is an index into the metadata hash table, so that the metadata's digital signature is the link to the metadata.

4. (Previously Presented) The method of claim 3, wherein at least one or both of the digital signatures is generated using a hashing algorithm.

5. (Previously presented) The method of claim 4, wherein the hashing algorithm is the SHAl secure hashing algorithm.

6. (Previously Presented) The method of claim 3, wherein the entry in the content hash table comprises the content data and the link to the metadata.

7. (Previously Presented) The method of claim 6, wherein the entry in the metadata hash table comprises the metadata and the link to the content data.

8. (Canceled).

9. (Previously Presented) The method of claim 3, wherein the location table is a location hash table, and wherein storing the location comprises the steps of:

generating a digital signature from the location; and

storing the original location in an entry in the location hash table, wherein the location's digital signature is an index into the location hash table, so that the location hash table is indexed in response to the original location by indexing with the location's digital signature.

10-22 (Canceled).

23. (New) A data processing system comprising at least one computer and one or more data sources that are either stand alone or networked, the data processing system for storing components of at least one file that was stored in a first environment at the one or more data sources, the data processing system utilizing code embodied within the data processing system configured to perform operations, the operations comprising:

obtaining content data and metadata relating to the original data of the at least one file, wherein the at least one file is stored in a first environment created on the one or more different mediums operating in the one or more different platforms;

in a second environment created on the one or more different mediums operating in the one or more different platforms and the target location, storing the content data and the metadata of the at least one file, wherein the content data is associated with the metadata, and wherein the second environment is different from the first environment;

obtaining an original location corresponding to the at least one file, the original location indicative of where the at least one file is stored in the first environment;

in the second environment, storing the original location in a location table, wherein the location table includes the following:

a link to the content data stored in a content hash table, indexed in response to the original location indicative of where the at least one file was stored in the first environment; and

a link to the metadata stored in a metadata hash table, indexed in response to the original location where the file was stored in the first environment;

reconstituting at least a piece of the at least one file by accessing at least one of the following in the location table:

the link to the content data, in response to the original location; and

the link to the metadata, in response to the original location; and

storing the content data in the content hash table and the metadata in ~~a~~ the metadata hash table, wherein the storing operation further comprises the steps of;

generating a digital signature from the content data; and

utilizing the digital signature to compare the content data of the least one file that is being extracted with content data already resident at the target location to avoid replication of content data and only storing content data that is not duplicative of the content data that is already resident at the target location.

24. (New) The data processing system of claim 23, wherein the operation of storing the content and metadata further comprises the operations of:

generating a digital signature from the metadata;

storing the content in an entry in the content hash table, wherein the content's digital signature is an index into the content hash table, so that the content's digital signature is the link to the content; and

storing the metadata in an entry in the metadata hash table, wherein the metadata's digital signature is an index into the metadata hash table, so that the metadata's digital signature is the link to the metadata.

25. (New) The data processing system of claim 24, wherein at least one or both of the digital signatures is generated using a hashing algorithm.

26. (New) The data processing system of claim 25, wherein the hashing algorithm is the SHAl secure hashing algorithm.

27. (New) The data processing system of claim 24, wherein the entry in the content hash table comprises the content data and the link to the metadata.

28. (New) The data processing system of claim 27, wherein the entry in the metadata hash table comprises the metadata and the link to the content data.

29. (New) The data processing system of claim 24, wherein the location table is a location hash table, and wherein storing the location comprises the operations of:

generating a digital signature from the location; and

storing the original location in an entry in the location hash table, wherein the location's digital signature is an index into the location hash table, so that the location hash table is indexed in response to the original location by indexing with the location's digital signature.

30. (New) A non-transitory computer readable medium including instructions configured to utilize code for storing information related to at least one file, wherein the code is

embodied within the data processing system, the code comprising instructions configured to perform operations including:

obtaining content data and metadata relating to the original data of the at least one file, wherein the at least one file is stored in a first environment created on the one or more different mediums operating in the one or more different platforms;

in a second environment created on the one or more different mediums operating in the one or more different platforms and the target location, storing the content data and the metadata of the at least one file, wherein the content data is associated with the metadata, and wherein the second environment is different from the first environment;

obtaining an original location corresponding to the at least one file, the original location indicative of where the at least one file is stored in the first environment;

in the second environment, storing the original location in a location table, wherein the location table includes the following:

a link to the content data stored in a content hash table, indexed in response to the original location indicative of where the at least one file was stored in the first environment; and

a link to the metadata stored in a metadata hash table, indexed in response to the original location where the file was stored in the first environment;

reconstituting at least a piece of the at least one file by accessing at least one of the following in the location table:

the link to the content data, in response to the original location; and

the link to the metadata, in response to the original location; and

storing the content data in the content hash table and the metadata in ~~a~~ the metadata hash table, wherein the storing operation further comprises the steps of;

generating a digital signature from the content data; and

utilizing the digital signature to compare the content data of the least one file that is being extracted with content data already resident at the target location to avoid replication of content data and only storing content data that is not duplicative of the content data that is already resident at the target location.

31. (New) The computer readable medium of claim 30, wherein the operation of storing the content and metadata further comprises the operations of:

generating a digital signature from the metadata;

storing the content in an entry in the content hash table, wherein the content's digital signature is an index into the content hash table, so that the content's digital signature is the link to the content; and

storing the metadata in an entry in the metadata hash table, wherein the metadata's digital signature is an index into the metadata hash table, so that the metadata's digital signature is the link to the metadata.

32. (New) The computer readable medium of claim 31, wherein at least one or both of the digital signatures is generated using a hashing algorithm.

33. (New) The computer readable medium of claim 32, wherein the hashing algorithm is the SHAl secure hashing algorithm.

34. (New) The computer readable medium of claim 31, wherein the entry in the content hash table comprises the content data and the link to the metadata.

35. (New) The computer readable medium of claim 34, wherein the entry in the metadata hash table comprises the metadata and the link to the content data.

36. (New) The computer readable medium of claim 31, wherein the location table is a location hash table, and wherein storing the location comprises the operations of:

generating a digital signature from the location; and

storing the original location in an entry in the location hash table, wherein the location's digital signature is an index into the location hash table, so that the location hash table is indexed in response to the original location by indexing with the location's digital signature.

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Bétit whose telephone number is (571)272-4075. The examiner can normally be reached on Monday through Friday 9:30 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on (571) 272-4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jacob F. Bétit/
Primary Examiner, Art Unit 2169

jfb
12 Sep 2011